対称式への応用

Joh @物理のかぎプロジェクト

2007-03-03

ここまでの結果の応用として，対称式へガロア理論を応用することを考えてみます．この後に続く議論への準備をも兼ねています．初めて読む人は，記号が少し複雑で分かりにくいという印象を持つと思います．そういうときは，二次方程式なり三次方程式なり，簡単な例を手元で計算しつつ，記号の意味を確認するようにしてみて下さい．分かってしまえば，そんなに難しい話ではありません．

基本対称式

一般に，体 F^n 上の n 変数多項式は次式のように表現できます．

$$f(x_1, x_2, ..., x_n) = \Sigma c(\nu_1, \nu_2, ..., \nu_n) x_{\nu_1}^1 x_{\nu_2}^2 \cdots x_{\nu_n}^n$$

ここで係数 $c(\nu_1, \nu_2, ..., \nu_n)$ は F^n の元で，ν_i は次数（正の整数）を表すとします．ある一つの項に関して，ν_i の和がその項の次数となります．いきなり一般の n 次の話から始めたので，少し記号がややこしく感じるかも知れませんが，$f(x, y, z) = x^2 + y^2 + z^2 - 2(xy + yz + zx) + xyz$ など，何でもいいので具体例を考えてみると記号の意味は明らかだと思います．

さて，この n 変数の多項式に対し，n 項の置換操作 $\sigma \in S_n$ を考えます．

$$\sigma f(x_1, x_2, ..., x_n) = f(\sigma(x_1), \sigma(x_2), ..., \sigma(x_n))$$

例えば，$\sigma = (1\ 2\ 3)$ と $f(x_1, x_2, x_3) = x_1^2 + x_2 x_3$ に対し，$\sigma f = x_2^2 + x_3 x_1$ となります．この例では f と σf が異なる多項式となってしまいました．これに対し，n 次の多項式で，S_n の全ての元に対して式全体が不変に保たれるものを **対称式** と呼びます．例えば，$\sigma = (1\ 2\ 3)$ に対して $f(x_1, x_2, x_3) = x_1 + x_2 + x_3$ は対称式です．

特に，基本対称式 μ と呼ばれるものは次のように定義されます．

$$(\xi - x_1)(\xi - x_2) \cdots (\xi - x_n) = \xi^n + \mu_1 \xi^{n-1} + ... + \mu_{n-1} \xi + \mu_n$$

具体的に幾つか書き下してみれば，既に見慣れた形であることに気づくでしょう．

$$\mu_1 = x_1 + x_2 + ... + x_n$$

$$\mu_2 = x_1 x_2 + x_1 x_3 + ... + x_{n-1} x_n$$

.....

$$\mu_n = x_1 x_2 \cdots x_n$$

theorem

体 F 上の n 次対称式は，基本対称式だけを使って一意的に表現できます．

この定理の証明は省略します．例えば対称式 $x_1^2 + x_2^2 + ... + x_2^n$ は，基本対称式を使って $\mu_1^2 - 2\mu_2$ と表せます．(この例は，手を動かしてみればすぐに確認できると思います．)

ガロア群と方程式の解

体 F 上の多項式 $f(x)$ を考えます．代数学の基本定理 によれば，$f(x)$ は少なくとも複素数体 C 上では一次式の積に因数分解可能なはずですが，実際は F と C の間に無数にある中間体のどこかで，一次式の積に因数分解可能になります．そのような分解体で最小のものを，最小分解体 と呼ぶのでした．

さて，ガロア拡大体について，次のような言い換えが可能でした．

Important

『 E は F のガロア拡大体です．』⇔『 E は，F 上のある分離多項式 $f(x)$ の最小分解体になっています．』

これを使って，次の定理を証明します．

theorem

$f(x)$ の解を $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ とします．ガロア群 $\mathcal{G}(E/F)$ の元は，$f(x)$ の解を置換します．

proof

ガロア群 $\mathcal{G}(E/F)$ の元 ϕ は F を固定体としますから，$0 = \phi(f(\alpha_i)) = f(\phi\alpha_i)$ がなりたちます．よって $\phi(\alpha_i)$ もやはり $f(x)$ の解で，$\{\alpha_1, \alpha_2, ..., \alpha_n\}$ のどれか一つに等しくなります．■

方程式のガロア群

体 F 上の方程式 $f(x)=0$ の最小分解体を E とします．このとき，$\mathcal{G}(E/F)$ を **方程式 $f(x)=0$ のガロア群** と定義します．以後，方程式論の文脈で『方程式のガロア群』と出てきたら，係数体と最小分解体に対するガロア群だと解釈して下さい．

ここでもう一つ，役にたつ定理を紹介します．

theorem

既約な n 次方程式 $f(x)=0$ のガロア群は，n 次対称群 S_n の部分群になります．

proof

既約な n 次方程式 $f(x)=0$ の解を置換する n 次の対称群を σ とします．ある解 α_i の置換 $\sigma(\alpha_i)$ もやはり解なのですから，$\sigma(\alpha_i)=\alpha_{\sigma(i)}$ と表現してもよいはずです．実際，$\sigma(\alpha_i)$ に $\alpha_{\sigma(i)}$ を対応させる写像は単準同型で，置換

$$\begin{pmatrix} 12...n \\ \sigma(1)\sigma(2)...\sigma(n) \end{pmatrix}$$

は S_n の部分群です．■

この定理の例として，$f(x)=x^3-2$ のガロア群を求めてみます．$\omega=\frac{-1+i\sqrt{3}}{2}$ と置くと，$f(x)=0$ の解 x は次のように表わされます．

$$x_1=\sqrt[3]{2},\quad x_2=\sqrt[3]{2}\omega,\quad x_3=\sqrt[3]{2}\omega^2$$

これより，$f(x)$ の最小分解体は $Q(\sqrt[3]{2},i\sqrt{3})$ で，拡大次数は 6 だと分かります．一般に $Q(\sqrt[3]{2},i\sqrt{3})$ の元が，$\xi=a_1+a_2\sqrt[3]{2}+a_3\sqrt[3]{2^2}+a_4i\sqrt{3}+a_5i\sqrt[3]{2}\sqrt{3}+a_6i\sqrt[3]{2^2}\sqrt{3}$ のように書けることを確認して下さい．また，ガロア群は今の定理より，S_3 に同型です．位数 $|S_3|=3!=6$ と拡大次数の関係も確認してください．

いま，Q と $Q(\sqrt[3]{2},i\sqrt{3})$ の中間体には $Q(\sqrt[3]{2})$ と $Q(i\sqrt{3})$ の二つが考えられます．$[Q(\sqrt[3]{2},i\sqrt{3}):Q(\sqrt[3]{2})]=3$, $[Q(\sqrt[3]{2},i\sqrt{3}):Q(i\sqrt{3})]=2$ となっています．

---

*1 実は，ガロアが一番最初にガロア群を考えたとき，固定体や拡大体の概念から入っていったのではなく，『方程式の解を置換する操作』を考えてガロア群の考えに至ったのです．ですから，この記事では，ガロア群は方程式の解を置換するという性質を定理として紹介しましたが，当初の発見的視野に戻れば，この性質をガロア群の定義と考えても良いのでしょう．先の見通しを良くするため，対称式を復習した理由や，この辺りの事情を補足しておきます．方程式には，解と係数の関係というものがありました．二次方程式の場合は $\alpha=a+b,\beta=ab$ などと書けることを中学か高校で習ったと思います．解は係数の対称式によって表現されていますが，解と係数の関係は，方程式を $(x-\alpha)(x-\beta)(x-\gamma)\cdots$ のような形に表現して展開して得られたものであることを考えれば，対称式になるのも当たり前のことです．解と係数の関係を逆に解けば，係数を解の対称式として表現することが出来ます．対称式ですから，解を置換したところで係数は不変のはずです．すなわち，係数体はこの置換に対し，固定体になっています．このような対称群を，ガロアは当初，方程式論の枠組みの中でガロア群として考えたのです．方程式が代数的に解ける条件をまだ紹介していませんので，これより先のことは説明できませんが，今までに勉強してきた，ガロア群，対称式，固定体などの概念を，この先どのように使うのかを概観しました．

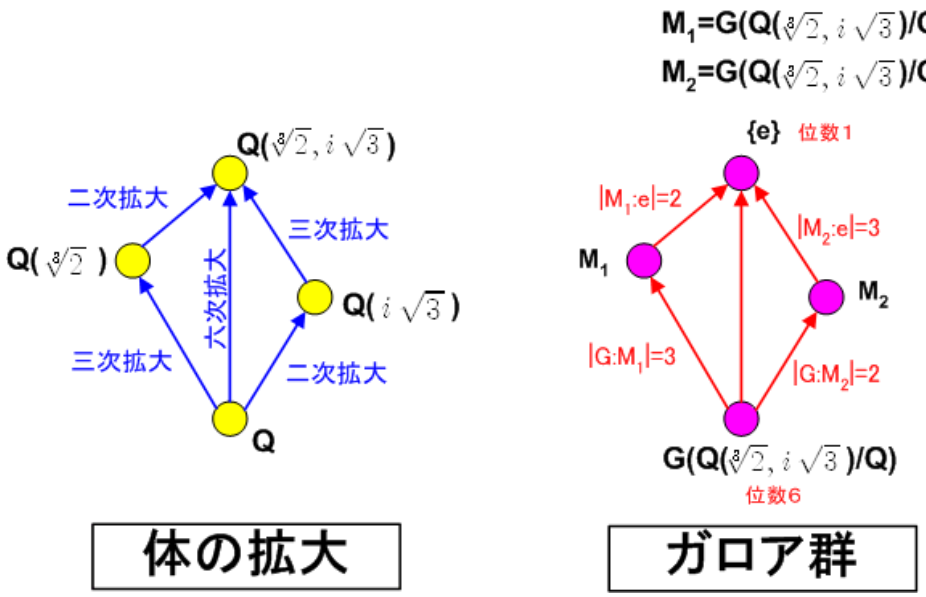
まず $Q(i\sqrt{3})$ の自己同型写像として，$\sqrt[3]{2}$ を $\sqrt[3]{2}\omega$ に移す写像を σ 考えます．

$$\begin{aligned}\sigma(\xi) &= a_1 + a_2\sqrt[3]{2}\omega + a_3\sqrt[3]{2^2}\omega^2 + a_4 i\sqrt{3} + a_5 i\sqrt[3]{2}\sqrt{3}\omega + a_6 i\sqrt[3]{2^2}\omega^2\sqrt{3} \\ &= a_1 + \frac{1}{2}a_2\sqrt[3]{2}(-1+i\sqrt{3}) + \frac{1}{2}a_3\sqrt[3]{2^2}(-1-i\sqrt{3}) + a_4 i\sqrt{3} + \frac{1}{2}a_5 i\sqrt[3]{2}\sqrt{3}(-1+i\sqrt{3}) + \frac{1}{2}a_6 i\sqrt[3]{2^2}\sqrt{3}(-1-i\sqrt{3}) \\ &= a_1 - (\frac{1}{2}a_2 + \frac{3}{2}a_5)\sqrt[3]{2} - (\frac{1}{2}a_3 + \frac{3}{2}a_6)\sqrt[3]{2^2} + a_4 i\sqrt{3} + \frac{1}{2}(a_2 - a_5)i\sqrt[3]{2}\sqrt{3} - \frac{1}{2}(a_3 + a_6)i\sqrt[3]{2^2}\sqrt{3}\end{aligned}$$

この写像は $a_1 + a_4 i\sqrt{3}$ の部分を不変に保ちますので，$Q(i\sqrt{3})$ の自己同型写像であり，σ は $\mathcal{G}(Q(\sqrt[3]{2}, i\sqrt{3})/Q(i\sqrt{3}))$ の元だと言えます．σ によって $f(x)$ の解は $x_1 \to x_2 \to x_3 \to x_1$ のように巡回的に置換されます．これに応じて $M_1 = \{e, \sigma\sigma^2\}$ も群をなし，$\mathcal{G}(Q(\sqrt[3]{2}, i\sqrt{3})/Q)$ の部分群となります．

次いで $i\sqrt{3}$ を $-i\sqrt{3}$ に移す写像 τ を考えます．τ は明らかに $Q(\sqrt[3]{2})$ の自己同型写像で，$\mathcal{G}(Q(\sqrt[3]{2}, i\sqrt{3})/Q(\sqrt[3]{2}))$ の元です．$\tau^2 = e$ に注意すると，τ $M_2 = \{e, \tau\}$ という群をなすことが分かります．これも $\mathcal{G}(Q(\sqrt[3]{2}, i\sqrt{3})/Q)$ の部分群です．

中間体とガロア群との対応関係を図にすると，次のようになります．拡大次数，ガロア群の位数，体とガロア群それぞれの包含関係に注意して下さい．



これらの結果と $\tau\sigma^2 = \sigma\tau$, $\sigma^2\tau = \tau\sigma$ に気をつけて，$\mathcal{G}(Q(\sqrt[3]{2}, i\sqrt{3})/Q) = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \tau\sigma\}$ が決まります．$\mathcal{G}(Q(\sqrt[3]{2}, i\sqrt{3})/Q)$ には M_1, M_2 の他に，$\{e\}$, $\mathcal{G}(Q(\sqrt[3]{2}, i\sqrt{3})/Q)$ には M_1, M_2 自身，そして $\sigma M_2\sigma$, $\sigma^2 M_2\sigma^2$ という合計六個の部分群があります．

先ほどの中間体とガロア群の対応関係を示す図に $\sigma M_2\sigma$ と $\sigma^2 M_2\sigma^2$ も書き込めば，さらに二本ずつ，線が増えることになります．